Amendment to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A method for providing security mobility between two cellular systems comprising:

requesting access to a first cellular system by a mobile device;

authenticating the mobile device by the first cellular system;

generating at least one second ciphering key for a second cellular system, the at least one second ciphering key generated by an interoperability authentication center ~~at a first~~at the first cellular system and ~~by a mobile~~by the mobile device separately, the generating being performed concurrently with the authenticating;

encrypting traffic between the mobile device and the first cellular system using at least one first ciphering key for the first cellular system;

approving a handoff of the traffic of the mobile device from the first cellular system to the second cellular system;

sending the at least one second ciphering key from the first cellular system to the second cellular system; and

performing handoff by the mobile device from the first cellular system to the second cellular system, traffic between the mobile device and the second cellular

system being encrypted using the at least one second ciphering key, wherein ciphering of the traffic is maintained during handoff,

wherein the authenticating comprises:

sending an authentication request including an International Mobile Subscriber Identity (IMSI) of the mobile device to the authentication center at the first cellular system;

generating authentication vectors by the authentication center, the authentication vectors including at least a value and an encrypted version of the value;

sending the value to the mobile device;

encrypting the value at the mobile device to create a response and sending the response to the first cellular system; and

comparing the response with the encrypted version at the first cellular system, the mobile device being authenticated if the response and the encrypted version are the same.

2. (original) The method according to claim 1, further comprising the interoperability authentication center storing security related algorithms and information for at least one cellular system including the second cellular system.

3. (original) The method according to claim 1, wherein the first cellular system comprises a Universal Mobile Telecommunications System (UMTS) system.

4. (original) The method according to claim 1, wherein the first cellular system comprises a Global System for Mobile Communications (GSM) system.

5. (original) The method according to claim 1, wherein the second cellular system comprises an Interim Standard (IS) 41 system.

6. (original) The method according to claim 5, wherein the at least one second ciphering key comprises a Signaling Message Encryption (SME) key and a Voice Privacy (VP) mask.

7. (original) The method according to claim 1, wherein the generating the at least one second ciphering key comprises using a Cellular Authentication and Voice Encryption (CAVE) algorithm.

8. (original) The method according to claim 7, wherein the CAVE algorithm uses at least one of an Authentication (A) key and Shared Secret Data (SSD) to generate the at least one second ciphering key, the A-key and the SSD used for authentication in the second cellular network.

9. (original) The method according to claim 1, wherein at least one first ciphering key is used in the generating at least one second ciphering key.

10. –12. (canceled)

13. (currently amended) The method according to ~~claim 12~~claim 1, further comprising generating the at least one first ciphering key for the first cellular system by the mobile device.

14. (currently amended) The method according to claim 1~~claim 12~~, wherein the at least one first ciphering key for the first cellular system is part of the authentication vectors.

15. (currently amended) The method according to claim 1~~claim 12~~, wherein the first sending and the second sending are performed by a Serving GPRS (General Packet Radio Service) Support Node (SGSN).

16. (currently amended) The method according to claim 1~~claim 12~~, wherein the authentication center comprises a Home Subscriber System (HSS).

17. (currently amended) The method according to claim 1~~claim 12~~, wherein the authentication center comprises a Home Subscriber System (HSS).

18. (currently amended) The method according to claim 1~~claim 12~~, wherein the generating at least one second ciphering key for a second cellular system occurs at the authentication center.

19. (currently amended) A method for providing security mobility between two cellular systems comprising:

requesting access to a first cellular system by a mobile device;

initiating an authentication of the mobile device;

generating at least one first ciphering key for a second cellular system, the at least one first ciphering key generated by an interoperability authentication center at the first cellular system and by the mobile device separately, the interoperability authentication center storing security related algorithms and information for at least one cellular system including the second cellular system;

~~authenticating the mobile device,~~encrypting traffic between the mobile device and the first cellular system ~~being encrypted~~ using at least one second ciphering key for the first cellular system;

approving a handoff of the traffic of the mobile device from the first cellular system to the second cellular system;

sending the at least one first ciphering key from the first cellular system to the second cellular system; and

performing handoff by the mobile device from the first cellular system to the second cellular system, traffic between the mobile device and the second cellular

system being encrypted using the at least one first ciphering key for the second cellular system, wherein ciphering of the traffic is maintained during the handoff

wherein the authenticating comprises:

sending an authentication request including an International Mobile Subscriber Identity (IMSI) of the mobile device to the authentication center at the first cellular system;

generating authentication vectors by the authentication center, the authentication vectors including at least a value and an encrypted version of the value;

sending the value to the mobile device;

encrypting the value at the mobile device to create a response and sending the response to the first cellular system; and

comparing the response with the encrypted version at the first cellular system, the mobile device being authenticated if the response and the encrypted version are the same.

20. (original) The method according to claim 19, wherein the first cellular system comprises a Universal Mobile Telecommunications System (UMTS) system.

21. (original) The method according to claim 19, wherein the second cellular system comprises an Interim Standard (IS) 41 system.

22. (original) The method according to claim 21, wherein the at least one first ciphering key comprises a Signaling Message Encryption (SME) key and a Voice Privacy (VP) mask.

23. (original) The method according to claim 19, wherein at least one second ciphering key is used in the generating at least one first ciphering key.

24. - 29. (canceled)

30. (currently amended) A system for providing security mobility between two cellular systems comprising:

at least one mobile device;

a first cellular network, the first network comprising:

at least one network element, the at least one network element authenticating each at least one mobile device desiring access to the first cellular network, traffic between the at least one mobile device and the first cellular system being encrypted using at least one first ciphering key for the first cellular network; and

an interoperability authentication center (IAuC), the IAuC storing security related algorithms and information for at least one cellular network, the IAuC capable of generating at least one second ciphering key for each at least one cellular

network, the at least one mobile device capable of generating the at least one second ciphering key for each at least one cellular network;

a gateway operably connected to the first cellular network;

a second cellular network operably connected to the gateway, the gateway transferring an at least one second ciphering key for the second cellular network from the first cellular network to the second cellular network before a handoff of the traffic from the first cellular network to the second cellular network, after handoff the traffic between the at least one mobile device and the second cellular system being encrypted using the at least one second ciphering key for the second cellular network, wherein ciphering of the traffic is maintained during handoff

wherein the authenticating comprises:

sending an authentication request including an International Mobile Subscriber Identity (IMSI) of the mobile device to the authentication center at the first cellular system;

generating authentication vectors by the authentication center, the authentication vectors including at least a value and an encrypted version of the value;

sending the value to the mobile device;

encrypting the value at the mobile device to create a response and sending the response to the first cellular system; and

comparing the response with the encrypted version at the first cellular system, the mobile device being authenticated if the response and the encrypted version are the same.

31. (original) The system according to claim 30, wherein the first cellular network comprises a Universal Mobile Telecommunications System (UMTS) system.

32. (original) The system according to claim 30, wherein the second cellular network comprises an Interim Standard (IS) 41 system.

33. (original) The method according to claim 30, wherein at least one first ciphering key is used in the generating at least one second ciphering key.